UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/829,499	04/22/2004	Cornell J. Kinderknecht	40003892-0056-002	6946

26263 7590 06/15/2009

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER	
VU, TUAN A	

ART UNIT	PAPER NUMBER
2193	

MAIL DATE	DELIVERY MODE
06/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/829,499	KINDERKNECHT ET AL.	
	Examiner	Art Unit	
	TUAN A. VU	2193	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the Applicant's response filed 4/08/09.

As indicated in Applicant's response, claims 1, 3, 10-14, 17-20, 22-27, 30-32 have been amended. Claims 1-33 are pending in the office action.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-6, 10-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Calder et al, USPubN: 2002/0092003(hereinafter Calder) in view of Graham et al, USPubN: 2002/0178271 (hereinafter Graham).

As per claim 1, Calder discloses a system for controlling an application process comprising:

an injector stored on a first computing device executing the application process (e.g. step 810, Fig. 8; para 0088, pg. 5 – Note: initializing package being transmitted – step 540 Fig. 5 – reads on injector code transmitted then stored in client application);

redirect code placed by the injector in a memory (e.g. interception module loaded … application package starts - para 0088,pg. 5; step 540 Fig. 5; Fig. 9**)** of the first computing device and

a library of redirect functions operable to be referenced by the redirect code during execution of the application process (e.g. step 920 - Fig. 9; para 0096, pg. 5; step 620,

interception module 810 -Fig. 8; para 0102-0103, pg. 6 – Note: implementing interception module with API that patches every loaded DLLs reads on library of redirect functions; i.e. patched DLLs), wherein the redirect code is operable to

(i) intercept at least one function call (para 0206-0297, pg. 14; para 0127, pg. 8) made by the application process (intercept 940 - Fig. 9; para 103, pg. 6; para 0127, pg. 8) to access secured data (e.g. sensitive data stored in databases … intercepts all … database access functions – para 0118, pg. 7; para 0127, pg. 8) and

(ii) execute at least one of the redirect functions in place of the at least one intercepted function call (e.g. step 990 - Fig. 9 ; modified binary 768 Fig. 7) so to enable the application process, executing at the first computing device, to access the secured data (Fig. 36-37 – Note: using a virtualized interface – application package 115, Fig. 2 -- with loaded libraries that are patched for intercepting application calls – see para 0145-0149, pg. 9-10 – and to virtualize the application call -- change a real DB entity invocation – step 3625, step 3635, Fig. 36 - to a virtual entity invocation reads on executing *in place of* original application function calls – see Fig. 18, 24 ,26, 27)

Calder does not explicitly disclose that *the secured data being accessed by the redirect function is at the remote computer system.* Calder discloses NW interconnectivity with socket calls among clients (Fig. 19-20) in a wide network and implementing client-side virtualized interface with specialized *patched libraries* (*application package 115* - Fig. 2; Fig. 16) to intercept communication calls in a multi-machines paradigm (client 140, 150, 160, server 120 – Fig. 100) where any client can communicate with other client/server machines (para 0077, pg. 4; *participating client* - para 0088, pg. 5) and where sensitive data in a given participating client

can be prevented from being directly accessed via using this interception module (para 0084-0086, pg. 5) whereby pertinent client application or system calls are redirected to a virtualized package including function calls and accessible set of "virtualized" DB data (step 830 – Fig. 8; Fig. 36). Based on the paradigm of participation of client and vendors alike, along with virtualized interface that enforces DB accesses (para 0118, pg. 7) or system calls (e.g. *system command ... vendor ... access a database* – para 0207, pg. 14) to be redirected to a client's virtualized copy of a true database (Fig. 36-37) whereby sensitive data belonging to each client can be verified for access (see *allowable list, key lookup* - para 0209-0215, pg. 14) the remote nature of each participating *vendor* or *client* respective to each other using the virtualization intercepting functionality (see Fig. 3-4) suggests that sensitive data can be stored as virtualized DB local to each client remote from each other -- or even a remote database accessible to each vendor (para 0207, pg. 14). According to the latter concept, practice such as maintaining a *remote database* in a trusted NW is evidenced in Graham (para 0080, pg. 6; *external database* - Fig. 14-16; Fig. 24) which teaches policy abiding intercommunication paradigm including wrapper component to redirect remote invocation and NW security rules checking. In light of the intercommunication paradigm wherein each client in its local environment contains sensitive data being virtualized based on a true value of a DB entity (see step 3625, step 3635, Fig. 36) and that sensitive data in such virtualized format exists in every participating client, it would have been obvious for one skill in the art at the time the invention was made to implement the interception module by Calder so *sensitive data* being virtualized for access (by any participating client) is stored in (a) any client remote from any other participating clients, or (b) a remote database –as in Graham – which is accessible via socket calls to all users where true DB data can

be virtualized in a separate environment on a participating paradigm enabling a virtualized sensitive data to be controllably and locally accessed using verification process as set forth above (see para 0209-0215, pg. 14; i.e. to validate whether a localized DB access call can be permitted using the access list and interception module implemented for each participating machine with respect to the other machine of the network). One would be motivated to do so to ensure that sensitive data stored remote at a common database (as in Graham) or individually in each participating enterprise clients, each remote to one another, to be securely protected, to extent secure usage of data by a large group of users while maintaining trustworthiness of data, and obviating extraneous interdiction/trap measures that would overburden firewall processes and policies enforcing resources by low-level operating systems (see Calder: para 0008-0014, pg. 1-2)

As per claims 2-4, Calder discloses wherein the injector is pushed to the first computing device (interception module - para 0096, pg. 5 Note: initializing package being transmitted to client – step 540 Fig. 5 – reads on injector code pushed onto client application) executing the application process; wherein the set of target function calls comprises socket function calls (e.g. Fig. 27); wherein the library of redirect functions comprises a dynamic link library (e.g. step 540-Fig.5; Fig. 9).

As per claim 5, Calder discloses: a secure environment having a plurality of resources (e.g. *resource request 1335* - Fig. 13); a firewall securing all access to the plurality of resources in the secure environment (e.g. Fig. 22-24, 26; para 0076 - pg. 4; Fig. 39-40; page permissions 1325 -Fig. 13, Fig. 14-15); and policy identifying the resources authorized for access by the first computing device (*access LAN* - para 0074, 0076, pg. 3-4; Fig. 39-40; para 0131-0132 - Note:

LAN, WAN and internal network based on access checking and encryption of data reads on policy to deny unauthorized intrusion).

Calder does not explicitly disclose access policy pushed to the first computing device identifying the resources authorized for access by the first computing device. Based on Calder electronic signing of transmitted package and decrypting at client end (para 0089, para 0092, pg. 5) and the rationale in claim 1 wherein proxy or firewalls can be in place as to filter or validate socket content or algorithm to disallow non-approved request (see Calder: *socket information* – para 0152-0154 pg. 10; *pre-defined list* - para 0130-0132, pg. 8-9) the security requirement for user to enter a session which is also shown in Graham (e.g. *session, authentication* - para 0074, 0097) entails a process for authenticating users (e.g. via a session authentication) for their right to access resources in a intranet under control of a firewall. It would have been obvious for one skill in the art at the time the invention was made to implement encrypted package in Calder so that they also contain meta-information regarding access policy (e.g. algorithm to uncode keys, or list of predefined keys, socket meta information, pre-defined list of approved connections) to access data in the scheme as intended by Calder to retrieve content or as in Graham's access of protected network data with enforcement of policy and rules (Graham: Fig 4-5; 14-16).

As per claim 6, Calder discloses wherein the application process comprises an application operable to communicate with the secure environment resources using an Internet transport protocol, the redirect code, and the redirect functions (e.g. Fig. 1-4; Fig. 9; para 103, pg. 6).

As per claim 10, Calder discloses a method for controlling an application process comprising:

pushing an injector to a first computing device enabled to execute the application process (refer to claim 2);

starting an execution of the application process (Fig. 9); interrupting the execution of the application process; injecting, via the injector, a redirect code into the application process (Fig. 10-11),

executing the redirect code in the application process to reference a redirect library of redirect functions so that upon resuming the execution of the application process (replace 115, 1160 – Fig. 11 Note: libraries of functions - refer to claim 1), the redirect code is operable to

(i) intercept at least one function call made by the application process to access secured data (refer to claim 1), and

(ii) execute at least one redirect function in place of the at least one function call so as to enable the application process executing on the first computing device, to access the secured data (refer to claim 1).

Calder does not explicitly disclose that *the secured data being accessed by the redirect function is at the remote computer system.* But this limitation has been addressed in claim 1.

As per claim 11, Calder discloses: starting the application process; interrupting the execution of the application process; and injecting the redirect code into a memory space of the application process (Fig. 10-11).

As per claim 12, Calder discloses starting the execution of the application process using a debug option (Note: patching a API with initializing – see Fig. 5 -- reads on debug option) and catching an exception thrown by the application process (see Fig 12-13 - Note: intercepting system call at low level – see Fig. 10 -- reads on catching a exception at such level); and wherein

injecting the redirect code comprises locating memory space in the application process; injecting the redirect code into the memory space of the application process and setting an instruction pointer to the redirect code (refer to Fig. 10; Fig. 15, 33, 41).

As per claim 13, Calder discloses starting the execution of the application process using a suspend option (Note: initializing a initial application with settings and patching read on suspend); and wherein injecting the redirect code comprises creating memory space in the application process; injecting the redirect code into the memory space of the application process and setting an instruction pointer to the redirect code (refer to claim 12).

As per claim 14, Calder discloses starting the execution of the application process using a suspend option; and wherein injecting the redirect code comprises creating memory space in the application process; injecting the redirect code into the memory, space of the application process; and use using a create remote thread function to execute the redirect code (refer to claim 13).

As per claim 15, Calder discloses wherein executing the redirect code comprises: loading the redirect library of redirect functions; determining a location of an import table replacement (Fig. 7, 10 - Note: import table, export table reads on table of routines to insert to memory for replacement) function in the redirect library; and executing the import table replacement function (table 920, 1010 -Fig. 9, 10).

As per claim 16, Calder discloses table including a dynamic link library (Fig. 9, 10-11 – refer to claim 1).

As per claim 17, Calder discloses executing the import table replacement function comprises: searching an import table of the application process for the set of target at least one

function call: and modifying the at least one function call to reference one or more redirect functions in the redirect library (Fig. 9, 10-11 and related text).

As per claim 18, Calder discloses wherein executing the import table replacement function comprises: searching dynamic link libraries of the application process for the at least one function call; and modifying file at least one function call to reference one or more redirect functions in the redirect library (e.g. para 0102, pg. 6).

As per claims 19, 21, Calder discloses receiving user information; authenticating the user information; access policy specifying resources accessible by a user associated with the user information to a device used by the user; executing redirect functions to enable a secured access to a plurality of resources via a firewall (refer to claim 5)

Calder does not explicitly disclose access policy pushed to the first computing device identifying the resources authorized for access by the first computing device. But this has been addressed in claim 5.

As per claim 20, refer to claim 3

As per claim 22, Calder discloses a method comprising:

receiving user information; authenticating the user information (Fig. 18-19); and upon authentication of the user information (refer to rationale in claim 5),

intercepting at least one function call made by the application process to access at least one of a plurality of secure resources at a remote computing system and

executing at least one redirect function in place of the at least one function call (refer to claim 1), so as to enable the application process, executing on a first computing device, to access the at least one secure resource (refer to claim 1)

For the limitation as to secure resources *at the remote computer system*, refer to rationale in claim 1.

As per claim 23, Calder discloses injecting a redirect code into file application process; and executing the redirect code in the application process to reference a redirect library of redirect function (refer to claim 10) ;

As per claims 24-27, refer to claim 11-14, respectively.

As per claims 28-31, refer to claim 15-18, respectively

As per claims 32-33, refer to claim 20-21, respectively.

4. Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Calder et al, USPubN: 2002/0092003, and Graham et al, USPubN: 2002/0178271; further in view of Thomas et al., USPN: 6,148,336 (hereinafter Thomas).

As per claim 7, Calder does not explicitly disclose wherein the application process comprises an *email* application. But GUI-based applications for which resources request are being fulfilled to support user's applications is disclosed (see Fig. 33-34; Fig. 47) in Calder's network of Lan users. Email represents a private means of communications among users and this is shown in Graham (para 0024, pg. 3) while users applications having interception of messages with insertion of special code to redirect to a proper validating or readdressing of message request is disclosed in Thomas's Web-based paradigm (e.g. Fig. 6; *library ... containing a plug-in* - col. 9, lines 6-40) wherein socket communications are inserted with a plug-in supported via a DLL container for redirection with proper binding and re-wrapping (see Fig. 9-10). Based on Thomas' approach to introduce a novel way for addressing IP address filtering drawback wherein Email is one such application involving such filtering concern (see col. 2), it

would have been obvious for one skill in the art to implement the application examination by Calder (see Fig. 33-34; *decrypt* - Fig. 39) so that the interception of LAN network messages via IP/TCP protocol via some dynamic application extension (such as plug-in as by Thomas -- see SUMMARY of Invention - col. 4-5) would be able examine the likes of Email message (as in Graham) content and resolve potential incompatibility issues by this extension service such as examining, blocking, modifying, decrypting and re-encrypting prior to providing a wrap-up binding process (see Thomas, col. 5) which also endeavored as set forth above by Calder.

As per claims 8-9, Calder does not disclose wherein the application process comprises a web browser application wherein the application process comprises a file transfer application. But applications with Winsock (see Thomas: see Fig. 1-6) or SSL as in Graham (see para 0076, pg. 5) such as in Windows platforms with provisioning of Dlls (see Calder para 0081-0082) was known OSI layers upon which standard file transfer and browser protocols would have founded to provide communications between users and services illustrated such as in Graham's browser methodology (see Graham: web server - para 0240-0241, pg. 17; HTTP/FTP- para 0271-0272, pg. 20) which is also suggested as pages in Calder (*application page* – Fig. 33). The limitation that applications be Email, or FTP or browser messages in light of the interception and redirection as taught by both Calder, Graham and Thomas would have been obvious for the same rationale as set forth above, because application like those require message transfer using a proper protocol, and the interception as purported by Calder or Thomas would support examination of such message internals to provide a modified and adjusted redirection as mentioned above in the respective endeavor by Calder/Graham and Thomas.

Response to Arguments

5. Applicant's arguments filed 4/08/09 have been fully considered but they are moot or not persuasive. Following are the Examiner's observation in regard thereto.

USC § 103 Rejection under Calder and Li:

(A) Applicant's arguments regarding 'access the secure data at the remote computer system' (Appl. Rmrks pg. 12-13) is considered moot because a new grounds of rejection has been necessitated to address the amended claim language.

USC § 103 Rejection under Calder/Li and Thomas:

(B) The observations regarding deficiencies of Calder and Li are deemed based on the new language being added to the claims, hence are considered not commensurate with the previous grounds of rejection, as set forth in section A.

The resubmitted claims, in all, will stand rejected as set forth in the Office Action.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tuan A Vu whose telephone number is (571) 272-3735. The examiner can normally be reached on 8AM-4:30PM/Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lewis Bullock can be reached on (571)272-3759.

The fax phone number for the organization where this application or proceeding is assigned is (571) 273-3735 (for non-official correspondence - please consult Examiner before using) or 571-273-8300 (for official correspondence) or redirected to customer service at 571-272-3609.

Any inquiry of a general nature or relating to the status of this application should be directed to the TC 2100 Group receptionist: 571-272-2100.
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Tuan A Vu/

Primary Examiner, Art Unit 2193

June 11, 2009